Application No.: 10/099,739

AMENDMENTS TO THE CLAIMS

1. (Original) A method for securing cached data in an enterprise environment, said method comprising the steps of:

processing a request to locate data in a query cache;

if said data can be located in said query cache, retrieving said data from said query cache, decrypting at least one encrypted portion of said retrieved data, and forwarding said decrypted portion and any remaining unencrypted portion of said retrieved data to a requesting client; and,

if said data cannot be located in said query cache, retrieving said data from a back-end data source over a computer communications network, forwarding said retrieved data to said requesting client, encrypting at least a portion of said retrieved data and storing in said query cache said encrypted portion and any remaining unencrypted portion.

2. (Original) The method of claim 1, wherein said encrypting and decrypting steps utilize an encryption key stored in a hardware security module (HSM).

3. (Original) The method of claim 1, wherein said processing step comprises:

locating within said request a key;

subjecting said key to a one-way hashing function; and,

comparing said hashed key to individual one-way hashed keys in said query cache, said comparison determining whether said data can be located in said query cache.

2

Application No.: 10/099,739

4. (Original) A method for securing cached data in an edge-deployed query cache, said method comprising the steps of:

configuring an encryption engine with an encryption system selected from the group consisting of a hardware security module (HSM), a software encryption module, or a combined hardware and software encryption system;

associating the edge-deployed query cache with said encryption engine; and,

configuring the edge-deployed query cache both to encrypt entries for storage in the edge-deployed query cache using said configured encryption engine the edge-deployed query cache retrieving said entries for storage from a back-end data source prior to said encryption, and also to decrypt entries retrieved from the edge-deployed query cache using said configured encryption engine.

5. (Original) A secured query cache system comprising:

a query cache disposed in an edge server; and,

an encryption engine communicatively linked to said edge server, said encryption engine having a configuration for encrypting entries to said query cache and decrypting entries retrieved from said query cache.

6. (Original) The secured query cache system of claim 4, wherein said encryption engine comprises:

a modular interface for accepting interchangeable encryption configurations, said configurations comprising one of a hardware security module, and a software encryption component.

3

Application No.: 10/099,739

7. (Original) The system of claim 6, wherein said encryption module implements the JAVA(.TM.) Cryptography Extension.

8. (Original) A machine readable storage having stored thereon a computer program for securing cached data in an enterprise environment, said computer program comprising a routine set of instructions for causing the machine to perform the steps of:

processing a request to locate data in a query cache;

if said data can be located in said query cache, retrieving said data from said query cache, decrypting at least one encrypted portion of said retrieved data, and forwarding said decrypted portion and any remaining unencrypted portion of said retrieved data to a requesting client; and,

if said data cannot be located in said query cache, retrieving said data from a back-end data source over a computer communications network, forwarding said retrieved data to said requesting client, encrypting at least a portion of said retrieved data and storing in said query cache said encrypted portion and any remaining unencrypted portion.

9. (Currently Amended) The machine readable storage of claim 8 [[9]], wherein said encrypting and decrypting steps utilize an encryption key stored in a hardware security module (HSM).

10. (Original) The machine readable storage of claim 8, wherein said processing step comprises:

locating within said request a key;

4

Application No.: 10/099,739

subjecting said key to a one-way hashing function; and,

comparing said hashed key to individual one-way hashed keys in said query cache, said

comparison determining whether said data can be located in said query cache.

5